CLOUD COMPUTING USING FOR VARIOUS CRYPTOGRAPHIC ALGORITHM

Ms. Monika
Assistant Professor
Department of Computer Science and IT
SSM College, Dinanagar

Abstract:

Cloud computing is the delivery of computing services over the web instead of keeping files on a proprietary disk drive or local memory device. Computing services can include servers, storage, databases, networking, and software. The main reason and great advantage for using the cloud are that the user can store and access the stored data in the cloud from anywhere anytime and getting all its services for a low cost. Despite, Security has always been a big concern with cloud computing because the customer does not directly maintain the information stored in the cloud. Cloud Computing Environment (CCE) provides several deployment models to represent several categories of cloud owned by organization or institutes. However, CCE provide resources to Cloud Users through several services like PaaS, SaaS, IaaS. Cloud Computing is a notion based on the concept of summing up physical resources and displaying them as an unacknowledged resource. It is a model for producing resources, for sorting out applications, and for manifesto-independent user access to services. Cloud can come in different types, and the services and the applications that possibly run on clouds may or may not be provided by a cloud service provider. There are two unique group of models namely deployment models and service models. Service models consists of IaaS , SaaS, PaaS . The Deployment or deployment model consists of Public Cloud, Private Cloud, Hybrid Cloud, Community Cloud, Cloud Computing has lots of distinct properties that make it very important. privacy seems to be anunique concern in cloud Various types of service models under cloud computing facilitate various levels of privacy services. We will get the minimum security in IaaS (Infrastructure as a Service) and most with a SaaS provider. In this paper, we will focus upon the reviewing and understanding cloud security issues by proposing crypto algorithms and effective measures so as to ensure the data security in cloud.

Keywords: Cloud Computing environment (CCE), Cryptography, Security Issues Privacy, Security Algorithms, Encryption, Decryption.

1. Introduction

In the paper author formulate on basis of Passive attacks contain an attacker actually listening on a community phase and attempting to examine touchy records as it travels. Passive attacks may be on-line (wherein an attacker reads traffic in actual-time) or offline (wherein an attacker without a doubt captures site visitors in real time and perspectives it later possibly after spending a while decrypting it). Energetic assaults

contain an attacker impersonating a purchaser or server, intercepting communications in transit, and viewing and/or modifying the contents before passing them directly to their meant vacation spot (or dropping them absolutely).

Cloud Computing is the delivery of computing services such as servers, storage, databases, networking, software, analytics, intelligence, and more, over the Cloud (Internet). Cloud Computing provides an alternative to the on-premises data center. With an on-premises data center, we have to manage everything, such as purchasing and installing hardware, virtualization, installing the operating system, and any other required applications, setting up the network, configuring the firewall, and setting up storage for data. After doing all the set-up, we become responsible for maintaining it through its entire lifecycle. Crypto cloud computing may be a new secure cloud computing design. It will give protection of data security at the system level, and permits users access to shared services handily and accurately. Crypto cloud computing protects individual's connections with the skin world. It will shield the private privacy with none delay of data exchange. . Symmetric contains algorithms like DES, AES, 3 DES and Blowfish algorithm. Asymmetric contains algorithms like RSA, Diffie- Hellman Key Exchange. Symmetric key and asymmetric key algorithms is used to encrypt and decrypt the data in cloud.

2. Cryptography: Security principles & Algorithms

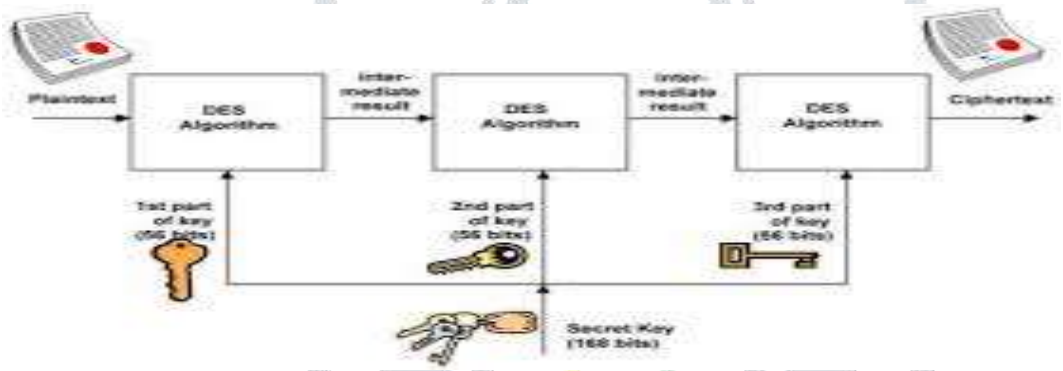
A comprehensive treatment of computer security technology, including algorithms, protocols, and applications. Covers cryptography, authentication, access control, database security, intrusion detection and prevention, malicious software, denial of service, firewalls, software security, physical security, human factors, auditing, legal and ethical aspects, and trusted systems. We have a various Algorithm's used in Cryptographic analysis and its security for cloud so that user can upload and Download their data on Cloud without any data damaging.

2.1 Symmetric keyalgorithms

Symmetric uses single key, which works for both encryption and decryption. The symmetric systems provide a two channel system to their users. It ensures authentication and authorization. Symmetric-key algorithms are those algorithms which uses only one and only key for both. The key is kept as secret. Symmetric algorithms have the advantage of not taking in too much of computation power and it works with very high speed in encryption. Symmetric-key algorithms are divided into two types: Block cipher and Stream cipher. In bock cipher input is taken as a block of plaintext of fixed size depending on the type of symmetric encryption algorithm, key of fixed size is applied on to block of plain text and then the output block of the same size as the block of plaintext is obtained. In Case of stream cipher one bit is encrypted at a particular time. Some popular Symmetric-key algorithms used in cloud computing includes: Data Encryption Standard (DES), Triple- DES, and Advanced Encryption Standard(AES).

a) DES :Data Encryption Standard

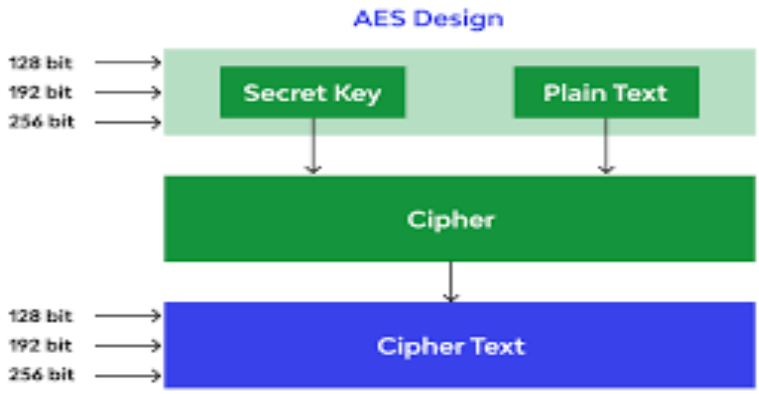
The most popular symmetric-key cryptography structure is the data Encryption device(DES). Encryption and decryption using the DES algorithm. Data Encryption standard: DES is that the archetypal block cipher-an algorithm that takes a fixed-duration string of plaintext bits and transforms it through a series of complicated operations into another CiphertextBitstring of the identical period. In case of DES, the block length is 64 bits. DES also uses a key to customize the transformation, so as that decryption can supposedly simplest be finished by means of who recognize the actual key used to encrypt. the important thing ostensibly includes sixty-four bits; but, the most convenient 56 of these are in point of fact utilized by the algorithm. eight bits are used totally for checking parity and are thereafter discarded. therefore the effective key period is fifty-six bits. The key's nominally stored or transmitted as 8 bytes, each with unusual parity. previous the principle rounds, the block is split into two 32-bit halves and processed alternately; this crisscrossing is noted because the Feistel scheme. The Feistel structure ensures that decryption and encryption are very similar tacticsthe only difference is that the subkeys are applied within the other order when decrypting.



b) Advanced Encryption Standard(AES)

In cryptography, the Advanced Encryption Standard **[3]** is type of symmetric-key encryption algorithm . Each of the ciphers has a 128-bit block size and having key sizes of 128, 192 and 256 bits, respectively. AES algorithm assures that the hash code is encrypted in a secure manner. AES has a block size of 128 Bits . Its algorithm is as follows: Key Expansion, Initial Round - Round Keys are added. Rounds, Sub Bytes—a non-uniformsubstitutionstepwhereeachbyteissubstituted with another according to a table. Rows are shifted—a transposition step where each row of the state is shifted cyclically a certain number of steps. Columns are mixed—a mixing operation which operates on the columns of the state, combining the four bytes in each column 8. Add RoundKey— each byte of that particular state is combined with the round key; each round key is derived from the given cipher key using a key schedule. Final Round, Sub Bytes, Shift Rows, Add Round Key. The DES algorithm was finally broken in 1998 using a system that costs about $250,000.Triple DES turned out to be too slow for efficiency as the DES algorithm was developed for mid-1970's hardware and did not produce efficient and effective software code. Triple DES has three times as many rounds as DES and is

correspondinglyslower

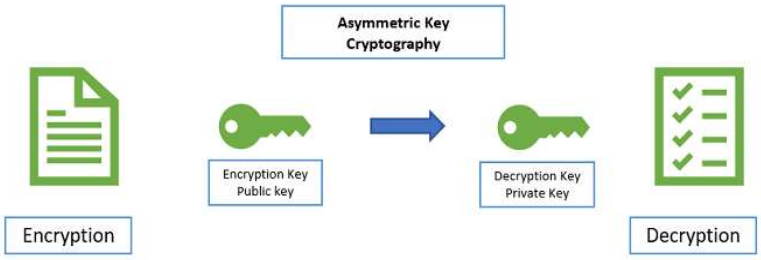


c) Blowfish Algorithm

Blowfish also comes under symmetric block cipher that can be used as a substitute for DES. It takes a variable-length key, starting from from 32 bits to 448 bits, making it considerably better for both domestic and exportable use. Blowfish was designed in 1993 by Bruce Schneier as a free, fast substiute to existing encryption algorithms. Since then it has been verified considerably, and it is gradually gaining popularity as a strong encryption algorithm. Blowfish is unpatented and license-free, and is available free for all uses.

2.2 Asymmetric Key Algorithms

Adleman and hence, it is termed as RSA cryptosystem. This algorithm is used for public-key cryptography and not private key cryptography. It is the first and still most commonly used asymmetric algorithm. It involves two keys namely a public key and a private key. The public key is used for encrypting messages and is known to everyone. Messages encrypted with the use of public key can be decrypted only by using the private key. In this verification process, the server implements public key authentication by signing a unique message with its private key, which is called as digital signature. The signature is then returned to the client. Then it verifies using the server's known public key.third party which officially declares that a particular public key belongs to a specific person or entityonly.an encryption key, referred to as his public key. Generally, this type of cryptosystem involves trusted referred to as his private key. Receiver needs to generate.decryption. This is a property which set this scheme different than symmetric encryption scheme. Each receiver possesses a decryption key of its own, generallycryptosystem. Different keys are used for encryption and It is relatively a new concept unlike symmetric.



Homomorphic encryption Algorithm:-

Is the conversion of data into Ciphertext that can be analyzed and worked with as if it were still in its original form.

Homomorphic encryptions allow complex mathematical operations to be performed on encrypted data without compromising the encryption. In mathematics, homomorphic describes the transformation of one data set into another while preserving relationships between elements in both sets. The term is derived from the Greek words for "same structure." Because the data in a homomorphic encryption scheme retains the same structure, identical mathematical operations -- whether they are performed on encrypted or decrypted data will yield equivalent results.

Homomorphic encryption is expected to play an important part in cloud computing, allowing companies to store encrypted data in a public cloud and take advantage of the cloud provider's analytic services.

Here is a very simple example of how a homomorphic encryption scheme might work in cloud computing:

1-Business XYZ has a *very important data set* (VIDS) that consists of the numbers 5 and 10. To encrypt the data set, Business XYZ multiplies each element in the set by 2, creatinga new set whose members are 10 and 20.

2- Business XYZ sends the encrypted VIDS set to the cloud for safe storage. A few months later, the government contacts.

3-Business XYZ and requests the sum of VIDS elements.

4-Business XYZ is very busy, so it asks the cloud provider to perform the operation. The cloud provider, who only has access to the encrypted data set, finds the sum of 10 + 20 and returns the answer 30.

5- Business XYZ decrypts the cloud provider's reply and provides the government with the decrypted answer, 15.

3. Security Problems Faced By Cloud Computing

When it comes to privacy and security, cloud is greatly affected by the threat of that. The people such as the vendors must make sure that the people using cloud does not face any problem such as data loss or theft of data. There is a chance where a malicious user or hacker can get into the cloud by impersonating a legitimate user, there by affecting the entire cloud thus affecting many people who are using the infected or affected cloud. Some of the problem which is faced by the Cloud computingare:

i. Datatheft
ii. Integrity ofdata
iii. Privacyproblems
iv. Loss ofdata
v. InfectedApplications
vi. Exact location ofdata
vii. Vendor levelSecurity
viii. User level Security

Major Security issues faced by Infrastructure as a Service be like:-

a) Cloud workloads and accounts being created outside of IT visibility (e.g., shadow IT)
b) Incomplete control over who can access sensitive data
c) Theft of data hosted in cloud infrastructure by malicious actor
d) Lack of staff with the skills to secure cloud infrastructure
e) Lack of visibility into what data is in the cloud
f) Inability to prevent malicious insider theft or misuse of data
g) Lack of consistent security controls over multi-cloud and on-premises environments
h) Advanced threats and attacks against cloud infrastructure
i) Inability to monitor cloud workload systems and applications for vulnerabilities
j) Lateral spread of an attack from one cloud workload to another

4. Conclusion and Future Scope

Cloud computing is growing as a new thing and it is the new trend indeed and many of the organizations and big companies are moving toward the cloud but lagging behind because of some security problems. Cloud security is an ultimate concept which will crush the drawbacks the acceptance of the cloud by the big MNCs, companies and organizations. There are a lot of security algorithms which may be implemented to the cloud. DES, Triple-DES, AES, and Blowfish etc are some symmetric algorithms. DES and AES are mostly used symmetric algorithms as they are relatively more secure. DES is quite simple to implement than AES.

But Homomorphic Encryption Algorithm is more powerful among all these algorithm mentioned above Homomorphism is a property by which a problem in one algebraic system can be converted to a problem in another algebraic system, be solved and the solution later can also be translated back effectively. Thus, homomorphism makes secure delegation of computation to a third party possible.

References:-

1- Swapnila S Mirajkar, SantoshkumarBiradar, “Enhance Security in Cloud Computing,” International Journal of Advanced Research in Computer Science and Software Engineering,2014. 13Ashalatha R, “A

survey on security as a challenge in cloud computing,"International Journal of Advanced Technology & Engineering Research (IJATER) National Conference on Emerging Trends

2- Douglas R. Stinson," Cryptography: Theory& Practice", Chapman and Hall Publications.

3- Cloud Performance Evaluation: Hybrid Load Balancing Model Based on Modified Particle Swarm Optimization and Improved Metaheuristic Firefly AlgorithmsJune 2020International Journal of Advanced Science and Technology 29(5):12315-12331, AdvinManhar

4- I. Agudo, D. Nuñez, G. Giammatteo, P. Rizomiliotis, and C. Lambrinoudakis, "Cryptography goes to the Cloud," Secure and Trust Computing, Data Management, and Applications, pp. 190-197: Springer, 2011.

5- T. K. Chakraborty, A. Dhami, P. Bansal, and T. Singh, "Enhanced public auditability & secure data storage in cloud computing." pp. 101-105.

6- B. Goswani, and D. S. Singh, "Enhancing Security in Cloud computing using Public Key Cryptography with Matrices," International Journal of Engineering Research and Applications, vol. 2, no. 4, pp. 339-344, 2012.

7- Sridevi, R. &Banupriya, C. B. (2017); A Survey on Cryptographic Cloud Storage Techniques, IJESRT, Vol. 6(7); pp. 602-605. DOI:10.5281/zenodo.829787

8- Narang, Ashima and Deepali Gupta. Different Encryption Algorithms in Cloud. April, 2018. ResearchGate.

9- Cyber Chief Magazine, Cybersecurity 2020 Top Trends Shaping Management Priorities, Ed 8.